Université de Rennes 1

Artihmétique des courbes elliptiques

Alice Bouillet/ Dorian Berger

Avril/Mai 2018

Table des matières

Introduction

Ce document est notre rapport sur le thème des courbes elliptiques, dans le cadre de notre Travail Encadré de Recherche, où l'on a été accompagnés par Mr Benoit Claudon.

La théorie des courbes elliptiques est un merveilleux mélange de mathématiques élémentaires, profondes et sophistiquées, qui se situe au croisement de multiples branches : arithmétique, géométrie algébrique, représentations de groupes, analyse complexe,... Historiquement, elles ont été introduites pour l'étude des équations diophantiennes et des courbes algébriques. On s'en sert également plus récemment en cryptographie, où l'on regarde les courbes elliptiques définies sur un corps fini.

Nous donnons ici une introduction au sujet et démontrons un résultat central de l'étude des points rationnels sur les courbes elliptiques, le théorème de Mordell, datant de 1922, qui stipule que le groupe (abélien) des points rationnels sur une courbe elliptique est de type fini : Il est donc isomorphe à un $\mathbb{Z}^r \times \frac{\mathbb{Z}}{q_1\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{q_2\mathbb{Z}}$ pour des certains $r, q_i \in \mathbb{Z}$ (Théorème de structure des groupes abéliens de type fini).

Sur $\mathbb{C}$, le groupe abélien $E(\mathbb{C})$ est isomorphe au quotient du groupe additif $\mathbb{C}$ par un réseau de $\mathbb{C}$, c'est-à-dire que la courbe n'est en fait qu'un tore. En effet, on montre que certaines courbes elliptiques sont paramétrées par la fonction de Weierstrass (qui dépend d'un réseau) puis ensuite qu'elles le sont toutes.

Nous commençons ici par rappeler quelques notions basique de géométrie algébrique, pour pouvoir ensuite aller au coeur de notre sujet.

1 Les courbes elliptiques

1.1 Quelques bases de géométrie algébrique

Dans toute cette section, on pose K un corps et $n \geq 1$ un entier.

Définition 1.1.1. *Soit $(P_i)_{i\in I}$ une collection d'éléments de $K[X_1, ..., X_n]$. On définit V un* ***ensemble algébrique affine*** *de la manière suivante :*

$$V := V((P_i)_{i\in I}) = \{(x_1, ..., x_n) \in \overline{K}^n, \forall i \in I, P_i(x_1, ..., x_n) = 0\}$$

Définition 1.1.2. *Une* ***courbe plane affine*** *sur K est définie de la manière suivante :*

$$C_f = V(f)$$

où f est un polynôme de $K[X, Y]$.

Définition 1.1.3. *Soit V un ensemble algébrique affine. On note $I(V)$ l'idéal suivant :*

$$I(V) = \{P \in K[X_1, ..., X_n] \mid \forall (x_1, ..., x_n) \in V, P(x) = 0\}$$

Définition 1.1.4. *Soit V un ensemble algébrique affine. On dit que V est* ***irréductible*** *si $I(V)$ est un idéal premier dans $\overline{K}[X_1, ..., X_n]$.*

Définition 1.1.5. *Un point $P = (x, y)$ d'une courbe $C = V_f$ est dit* ***singulier*** *si $(\frac{\partial f}{\partial X}(P), \frac{\partial f}{\partial Y}(P)) = (0, 0)$.*

Exemple 1.1.1. *Un point d'intersection de deux composantes irréductible d'une courbe est toujours singulier. En effet, prenons par exemple C_f où $f = f_1 f_2$ et $f_1(0, 0) = 0 = f_2(0, 0)$. Alors,*

$$\frac{\partial F}{\partial X}(0, 0) = \left(f_1 \frac{\partial f_2}{\partial X} + f_2 \frac{\partial f_1}{\partial X}\right)(0, 0) = 0$$

$$\frac{\partial F}{\partial Y}(0, 0) = \left(f_1 \frac{\partial f_2}{\partial Y} + f_2 \frac{\partial f_1}{\partial Y}\right)(0, 0) = 0$$

Définition 1.1.6. *On définit :*

$$C_f(K) = \{(x, y) \in K^2 \mid f(x, y) = 0\}$$

*l'ensemble des K-**points rationnels** de C_f.*

Passons maintenant à la partie projective.

Définition 1.1.7. ***L'espace projectif*** *de dimension n sur K est :*

$$P^n = \{(x_1, ..., x_{n+1}) \in \overline{K}^{n+1} \mid (x_1, ..., x_{n+1}) \neq (0, ..., 0)\}/\sim$$

où $(x_1, ..., x_{n+1}) \sim (x'_1, ..., x'_{n+1})$ si et seulement si $\exists c \in \overline{K}^*$ telle que $(x_1, ..., x_{n+1}) = (cx'_1, ..., cx'_{n+1})$.
On notera $[x_1 : ... : x_{n+1}]$ la classe de $(x_1, ..., x_{n+1})$ dans P^n.

Définition 1.1.8. *Un* ***isomorphisme projetif*** *de P^n dans P^n est le quotient par la relation d'équivalence d'un isomorphisme linéaire de K^{n+1}.*

Remarque 1.1.1. *Un isomorphisme f de K^{n+1} passe bien au quotient car $\forall \lambda \in K$, $f(\lambda x) = \lambda f(x)$, $\forall x \in K^{n+1}$, et de plus l'unique antécédent de 0 par f est 0.*

Comme nous allons maintenant travailler sur des quotients, nous devons nous assurer que les polynômes avec lesquels nous travaillons peuvent également passer au quotient. C'est la motivation de la définition suivante :

Définition 1.1.9. *Soit F un polynôme de $K[X_1, ..., X_n]$. On dit que F est* ***homogène*** *de degré d si $\forall \lambda \in K$, $F(\lambda X_1, ..., \lambda X_n) = \lambda^d F[X_1, ..., X_n]$.*

Définition 1.1.10. *Soit $P = [x : y : z]$ un point de P^2. Soit F un polynôme de $K[X, Y, Z]$. On dit que P est un* ***zéro*** *de F si $F(P) = 0$, c'est-à-dire si $F(\lambda x, \lambda y, \lambda z) = 0$ $\forall \lambda \in K$.*

On voit donc ici que lorsque P est un polynôme homogène, la nullité de P en un point de l'espace projectif ne dépend pas du représentant choisi.

Définition 1.1.11. *Soit $(P_i)_{i \in I}$ une collection de polynômes homogènes de $K[X_1, ..., X_{n+1}]$. On définit V un* ***ensemble algébrique projectif*** *de la manière suivante :*

$$V := V((P_i)_{i \in I}) = \{[x_1 : ... : x_{n+1}] \in P^n \mid \forall i \in I, P_i([x_1 : ... : x_n]) = 0\}$$

Définition 1.1.12. *Une* ***courbe projective plane*** *sur K est définie de la manière suivante :*

$$C_F = V(F)$$

où F est un polynôme homogène de $K[X, Y, Z]$.

Définition 1.1.13. *Soit V un ensemble algébrique projectif. On note $I(V)$ l'idéal suivant :*

$$I(V) = \{P \in K[X_1, ..., X_n] \mid \forall [x_1, ..., x_n] \in V, P(x) = 0\}$$

Définition 1.1.14. *Soit V un ensemble algébrique projectif. On dit que V est* ***irréductible*** *si $I(V)$ est un idéal premier dans $\overline{K}[X_1, ..., X_n]$.*

Définition 1.1.15. *Une **cubique** est une courbe projective plane où le F correspondant est un polynôme homogène de degré 3.*

Définition 1.1.16. *Un point P d'une cubique $C = V_F$ est dit **singulier** si $(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)) = (0, 0, 0)$.*

Remarque 1.1.2. *Cette définition est bien définie : elle ne dépend pas du représentant que l'on utilise. En effet si F est homogène de degré d, alors $\frac{\partial F}{\partial X_i}$ est homogène de degré $d-1$, $\forall i$.*

Définition 1.1.17. *On définit :*

$$C_F(K) = \{[x : y : z] \in P^2(K) \mid F(X, Y, Z) = 0 \text{ et } (x, y, z) \in K^3\}$$

*l'ensemble des K-**points rationnels** de C_F.*

Définition 1.1.18. *Soit C une courbe projective plane. Un **point à l'infini** de C est un point $P = [x : y : 0] \in C$, avec $(x, y) \in \overline{K}$.*

Définition 1.1.19. *Soit C une courbe projective plane, et $P \in C$ un point non singulier. Alors, la tangente à la courbe C au point P est donnée par :*

$$\frac{\partial F}{\partial X}(P)(X - X_P) + \frac{\partial F}{\partial Y}(P)(Y - Y_P) + \frac{\partial F}{\partial Z}(P)(Z - Z_P) = 0$$

Théorème 1.1.1. *(Théorème de Bezout)*
Deux courbes algébriques projectives sur un corps algébriquement clos, sans composantes communes, respectivement de degrés n et p (i.e où les polynômes homogènes correspondants sont de degrés n et p) possèdent exactement np points d'intersection, comptés avec leur multiplicité.

Corollaire 1.1.1. *Une droite coupe une cubique en exactement trois points.*

1.2 Passage du projectif à l'affine et réciproque

Proposition 1.2.1. *L'espace projectif P^n est couvert par les ensembles $U_i = \{[x_1 : ... : x_n] \mid x_i \neq 0\}$, et chaque U_i est en bijection avec K^n.*
Le complémentaire de U_i dans P^n est l'espace linéaire $\pi(H_i)$, où H_i est l'hyperplan d'équation $x_i = 0$ dans k^{n+1}, et π est la projection canonique de k^{n+1} dans P^n.

Démonstration. L'espace projectif est couvert par les U_i par définition.
Maintenant, on pose :

$$\Phi_i : K^n \to U_i \subsetneq P^n$$

$$(x_1, ..., x_n) \mapsto [x_1 : ... : x_{i-1}, 1, x_i : ... : x_n]$$

On trouve facilement son inverse :

$$\Phi_i^{-1} : U_i \to K^n$$

$$[x_1 : ... : x_i : ... : x_n] \mapsto (\frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i})$$

□

Définition 1.2.1. *Soit $P = P(X, Y) \in K[X, Y]$. On appelle $\overline{P}$* ***l'homogénéisé*** *de P défini ainsi :*

$$\overline{P}(X, Y, Z) = Z^d P(X/Z, Y/Z)$$

où d est le degré de P.

Exemple 1.2.1. *Soit $P(X, Y) = Y^2 + XY^3 + X^2Y + 3X$, alors $\overline{P}(X, Y, Z) = Z^2Y^2 + XY^3 + ZX^2Y + 3Z^3X$.*

Définition 1.2.2. *Soit $P(X, Y, Z)$ un polynôme homogène de $K[X, Y, Z]$. On appelle le* ***déshomogénéisé*** *de P le polynôme suivant :*

$$\tilde{P}(X, Y) = P(X, Y, 1)$$

Définition 1.2.3. *Soit $V = V((P_i)_{i\in I})$ un ensemble algébrique affine de K^n, que l'on voit en tant que sous ensemble de P^n grâce à l'application Φ_{n+1}. On définit la* ***clôture projective*** *de V, noté $\overline{V}$, l'ensemble algébrique projectif suivant :*

$$\overline{V} = \{P \in P^n \mid \overline{P_i}(P) = 0 \ , \ \forall i \in I\}$$

Regardons maintenant le cas qui nous intéresse : les courbes.

Proposition 1.2.2. *Soit H l'hyperplan $\{Z = 0\}$ (appelé ici "plan à l'infini"). Il y a une correspondance bijective entre les courbes algébriques irréductibles dans $\bar{k}^2$ et les courbes projectives irréductibles de P^2, non contenues dans H.*

$$\{\textit{Courbes affines non vide}\} \to \{\textit{Courbes projectives non contenues dans } H\}$$

$$C \mapsto \overline{C}$$

$$\tilde{C_F} \leftarrow C_F$$

où $\tilde{C_F}$ est la courbe définie par $f = F(X, Y, 1)$

Démonstration. Soit C_f une courbe affine. Soit g le polynôme qui la définie. On a $\overline{C} = \{[x : y : z] \in P^2 \mid \overline{g}([x : y : z]) = 0\}$ avec
$\overline{g}(X, Y, Z) = Z^d g(X/Z, Y/Z)$. Si $\overline{C}$ est contenue dans $Z = 0$, alors g est forcément constant, car s'il dépendait d'une variable X ou Y (ou les deux !), en posant $Z = 1$, on obtiendrait un polynôme non constant et donc il aurait une racine dans $\overline{k}$. Ainsi, comme la courbe C est supposée non vide, $\overline{C}$ n'est pas contenue dans $Z = 0$.
Montrons que $\tilde{\overline{C}} = C$. On a :

$$\overline{g}(X, Y, 1) = (Z^d g(X/Z, Y/Z))(X, Y, 1) = g(X, Y)$$

Donc $\tilde{\overline{C}} = C$.
Soit C une courbe projective non contenue dans $Z = 0$. Soit F son polynôme. Alors, comme précédemment, le polynôme F qui la définie n'est pas de la forme cZ^d. On a :

$$\overline{F(X, Y, 1)} = F$$

car Z n'est pas facteur de F car $I(C)$ est premier et donc comme ici $I(C) = (F)$, on a que F est irréductible. Ainsi, $\tilde{\overline{C}} = C$
On a donc bien une bijection. □

1.3 Premières définitions de courbes elliptiques

Définition 1.3.1. *Une **cubique lisse** ou **non singulière** est une cubique sans point singulier.*

Remarque 1.3.1. *Sur une cubique lisse, tout point admet une tangente.*

Proposition 1.3.1. *Soit $F \in K[X, Y, Z]$ un polynôme homogène. Alors,*

$$C_F \text{ n'a pas de point singulier } \Rightarrow F \text{ est sans facteur carré dans } \overline{K}[X, Y, Z]$$

Démonstration. Supposons que F ai un facteur carré dans $\overline{K}[X, Y, Z]$. Alors on écrit $F = (F_1)^2 F_2$, avec F_1 non constant. Alors F, $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ et $\frac{\partial F}{\partial Z}$ ont F_1 en facteur commun, et donc si on prend une racine de F_1, on obtient un point singulier. □

Définition 1.3.2. *Une **courbe elliptique** sur K est un couple (E, O) où E est une cubique lisse dont le polynôme est à coefficients dans K et O est un point K- rationnel de E. On nomme O l'origine.*

Exemple 1.3.1. *Ceci est une courbe elliptique : $y^2 = x^3 + x$, munie du point $[0 : 1 : 0]$.*

Exemple 1.3.2. *Ceci n'est pas une courbe elliptique : $y^2 = x^3$: Il y a une singularité en $(0, 0)$.*

Notation 1.3.1. *Si E est une courbe elliptique dont le polynôme est à coefficient dans un corps K, on la notera E/K.*

1.4 Mise sous forme de Weierstrass

Rappel 1.4.1. *Soit $F \in K[X, Y, Z]$. La **matrice Hessienne** associée à F est définie ainsi :*

$$\begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial Y \partial X} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial Z \partial X} & \frac{\partial^2 F}{\partial Z \partial Y} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}$$

Définition 1.4.1. *Soit C une cubique. Un point $P \in C$ non singulier est appelé **point d'inflexion** de C si la tangente à C en P intersecte C en P avec une multiplicité égale à 3.*

Proposition 1.4.1. *Soit C une cubique lisse sur K. Soit P un point d'inflexion de C. Alors, avec un changement de variables linéaire inversible avec ses coefficients dans K, on peut transformer P en $[0 : 1 : 0]$, et la tangente en ce point peut être transformée par $Z = 0$.*

Démonstration. La forme générale du polynôme qui définit la cubique est

$$F(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3$$

Soit $P = [x_P, y_P, z_P]$. Soit L la tangente à C en P. Comme P est un point d'inflexion, la multiplicité d'intersection de L et C en P est 3.
Soit $Q = [x_Q, y_Q, z_Q] \in L \backslash C$. Les vecteurs colonnes (x_P, y_P, z_P) et (x_Q, y_Q, z_Q) sont linéairement indépendants car P et Q sont deux points distincts du plan projectif. On complète cette famille avec le vecteur C en une base de K^3, grâce au théorème de la base incomplète. On obtient la matrice M suivante : $\begin{pmatrix} x_Q & x_P & \\ y_Q & y_P & C \\ z_Q & z_P & \end{pmatrix}$ M est bien sur inversible, soit M^{-1} son inverse. M^{-1} envoie P sur le point $[0:1:0]$ et Q sur le point $[1:0:0]$. Alors, M^{-1} envoie L sur la droite $Z = 0$, car par deux points projectifs passe une unique droite projective et l'unique droite passant par $[0:1:0]$ et $[1:0:0]$ est $Z = 0$. □

Proposition 1.4.2. *Soit C une cubique. Soit P un point non singulier de C. Alors, P est un point d'inflexion si et seulement si* $\det(H(F))(P) = 0$ *où H est la matrice hessienne associée à F.*

Remarque 1.4.1. *-Un calcul direct montre que le déterminant d'une cubique* ***lisse*** *est de degré exactement 3.*
-La condition $det(H) = 0$ est préservée par un changement de variables inversible.

Proposition 1.4.3. *Une cubique lisse possède 9 points d'inflexion, comptés avec multiplicité.*

Démonstration. On cherche ici des points qui annulent le polynôme, et le déterminant de la matrice Hessienne. On cherche donc les zéros communs de deux polynômes de degrés 3 : Il y en a donc 9, comptés avec multiplicité grâce au théorème de Bezout. □

Théorème 1.4.1. *Soit C une cubique lisse sur K. Soit O un point d'inflexion de C. Si le point $O = [0:1:0]$, et la tangente en ce point à C est $Z = 0$, alors la courbe C est de la forme :*

$$Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

avec les $a_i \in K$.
Cette forme est appelée ***Forme de Weierstrass*** *de la cubique C.*

Remarque 1.4.2. *-Sur la courbe définie par cette forme de Weierstrass, nous avons un point à l'infini : $[0:1:0]$, dans la représentation affine, cela correspond au point (∞, ∞).*
-L'équation affine correspondante est

$$Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$$

Démonstration. Soit maintenant $G = aU^3 + bU^2V + cUV^2 + dV^3 + eU^2W + fUVW + gV^2W + hUW^2 + iVW^2 + jW^3$ le polynôme définissant cette cubique. Montrons que certains de ces termes sont nuls.
On a $G([0:1:0]) = 0$ donc $d = 0$.
La tangente en $[0:1:0]$ est $W = 0$, donc $\frac{\partial G}{\partial U}([0:1:0]) = c = 0$ mais $\frac{\partial G}{\partial W}([0:1:0]) = g \neq 0$.
Les points d'intersection entre la courbe $\{G = 0\}$ et $\{W = 0\}$ vérifient $U^2(aU + bV) = 0$. Or, $[0:1:0]$ est un point d'inflexion donc cette équation n'a que ce point comme solution. Cela nous donne que $b = 0$ et $a \neq 0$.
Puisque une courbe projective est un polynôme modulo multiplication par un facteur non nul, on choisit comme représentant de G celui ayant un coefficient 1 devant U^3 (ceci est possible car $a \neq 0$).
On obtient alors un polynôme de la forme

$$G(U, V, W) = U^3 + aU^2W + bUVW + cV^2W + dUW^2 + eVW^2 + fW^3$$

Enfin, comme $c \neq 0$, on peut effectuer un nouveau changement de variable en posant $\lambda(U, V, W) = (U, V, \frac{-W}{c})$ et on obtient G sous forme de Weierstrass. □

Remarque 1.4.3. *Soit C une courbe elliptique, mise sous forme de Weierstrass. Soit $F = ZY^2 + a_1XYZ + a_3YZ - X^3 - a_2X^2Z - a_4XZ - a_6Z$ son polynôme. Regardons les points $[x:y:z]$ de cette courbe. Si $z = 0$, alors $x = 0$ et on obtient alors un unique point $[0:1:0]$. Si $z \neq 0$, on peut prendre $z = 1$ et alors on a que $[x:y:1] \in C_F \Leftrightarrow (x, y) \in C_f$ où $f = F(X, Y, 1)$.*

Théorème 1.4.2. *Si $Car(k) \neq 2, 3$, on peut toujours mettre une courbe elliptique sous forme de Weierstrass réduite, c'est-à-dire sous la forme suivante :*

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

avec $\Delta = 27b^2 + 4a^3 \neq 0$

Remarque 1.4.4. *La condition $\Delta = 27b^2 + 4a^3 \neq 0$ assure que la courbe est lisse. En effet, si on repasse dans le monde affine, l'équation devient :*

$$y^2 = x^3 + ax + b$$

On a alors, $\frac{\partial F}{\partial Y} = 2Y$ donc pour avoir un point singulier $P = (x, y)$, on a forcément que $y = 0$ car $Car(k) \neq 2$ et alors on obtient que x est racine de $x^3 + ax + b = 0$ et de sa dérivée, x est donc racine double de ce polynôme donc le discriminant de ce polynôme est nul, ce qui donne le résultat. Maintenant,si $z = 0$,on a $x = 0$ et donc $y = 1$ et $\frac{\partial F}{\partial Z}[0:1:0] \neq 0$ et donc ce point n'est pas singulier.

Démonstration. Soit $C = V(F)$ une courbe elliptique mise sous forme de Weierstrass, c'est-à-dire où $F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$ On effectue le changement de variable suivant :

$$X' = X \ , \ Y' = Y + \frac{a_1}{2}X \ , \ Z' = Z$$

On élimine ainsi le terme en XYZ. On continue en effectuant ce changement de variable :

$$X' = X + \frac{a_2}{3} \ , \ Y' = Y + \frac{a_3}{2} \ , \ Z' = Z$$

Ceci élimine les termes en X^2 et en Y. □

Exemple 1.4.1. *Soit $d \in \mathbb{Z}$, $d \neq 0$. Soit E la courbe elliptique donnée par l'équation*

$$X^3 + Y^3 = dZ^3$$

avec $O = [1, -1, 0]$. E est bien lisse car le seul point qui annule les dérivés partielles est $[0 : 0 : 0]$, qui n'est pas dans le plan projectif.
On veut trouver une équation de Weierstrass pour E. On utilise ce changement de variable :

$$\Phi([X : Y : Z]) = [12dZ : 36d(X - Y) : X + Y] := [x : y : z]$$

on obtient alors le polynôme

$$zy^2 = x^3 - 432d^2z^3$$

Φ est bien inversible, son inverse étant donnée par

$$\Phi^{-1}([x : y : z]) = [\frac{36dz + y}{72d} : \frac{36dz - y}{72d} : \frac{x}{12d}]$$

.

1.5 Loi de groupe sur les courbes elliptiques : Tangentes et cordes

Un des résultats les plus beaux sur les courbes elliptiques est le suivant : une courbe elliptique peut être dotée d'une structure de groupe abélien.

Définition 1.5.1. *On peut définir **une loi** sur une courbe elliptique (E, O). Soient P, Q deux points distincts de E. La droite joignant P à Q coupe la cubique en un troisième point (Théorème de Bezout). Soit R le troisième (éventuellement égal à P ou Q). On note $R = P \circ Q$. Si $P = Q$, on effectue la même opération avec la tangente de C en P. On définit alors l'addition en utilisant le point origine $O \in E(K)$, puis en posant $O' = O \circ O$ et enfin*

$$P + Q := O \circ (P \circ Q)$$

et

$$-P := O' \circ P$$

Théorème 1.5.1. *La loi définit précédemment est une* ***loi de groupe*** *sur la courbe elliptique, dont l'élément neutre est O. La cubique munit de cette loi est un groupe abélien.*

Démonstration. -Montrons tout d'abords que la loi est bien définie. Soient $P, Q \in E$. Par construction, $P \circ Q \in E$ et ainsi, $P + Q = O \circ (P \circ Q) \in E$ également. La loi est donc bien une loi de composition interne.
-Montrons que la loi est commutative. On a $P+Q = O\circ(P\circ Q) = O\circ(Q\circ P) = Q + P$.
-Montrons que O est un élément neutre. $P + O = O \circ (P \circ O) = O \circ R = P$ car R est le troisième point d'intersection de la courbe avec la droite (OP).
-Montrons que $P + (-P) = O$. Pour cela, regardons la construction du point $-P$. On trace la tangente en O, elle recoupe la cubique en O'. La droite (PO') recoupe la cubique en un point qui est $-P$. Vérifions que cette construction nous donne bien des opposés. Additionnons P et $-P$. Pour ce faire, prenons le troisième point d'intersection de la courbe avec la droite passant par P et $-P$: c'est O'. Maintenant, joignons O' et O et prenons à nouveau le troisième point d'intersection $O' \circ O$: c'est O car la droite passant par O et O' est la tangente à la courbe en O, elle passe donc "une fois par O' et "deux fois" par O. Ainsi, $P + (-P) = O$.
-Pour montrer l'associativité, nous avons besoin d'un lemme.

Soient $A, B, C \in E$. On pose :

$$A \circ B = D \ , \ A + B = G$$

$$B \circ C = U \ , \ B + C = V$$

$$A \circ V = W \ , \ G \circ C = F$$

$$l(X, Y, Z) \text{équation de la droite passant par} A, B, D$$

$$m(X, Y, Z) \text{équation de la droite passant par} G, C, F$$

$$n(X, Y, Z) \text{équation de la droite passant par} O, U, V$$

$$r(X, Y, Z) \text{équation de la droite passant par} A, W, V$$

$$s(X, Y, Z) \text{équation de la droite passant par} B, C, U$$

$$t(X, Y, Z) \text{équation de la droite passant par} D, G, O$$

Montrer l'associativité revient à montrer que F et W sont le même point qui est l'intersection r et m car $A + (B + C) = A + V = O \circ W$ et $(A + B) + C = G + C = O \circ F$.

F

Théorème 1.5.2. *Soient C' et $C"$ deux cubiques, sans composante commune, qui se coupent en neuf points distincts. Toute cubique qui passe par huit de ces points passe par le neuvième.*

Corollaire 1.5.1. *Si une cubique C intercepte deux cubiques C' et $C"$ sans composantes communes, chaque fois en 9 points distincts, et si 8 de ces points sont les mêmes, alors le neuvième point d'intersection est aussi le même.*

Démonstration. Soit C une telle cubique. On note

$$C \cap C' = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P\}$$

$$C \cap C" = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, Q\}$$

$$C' \cap C" = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, R\}$$

Comme C passe par les 8 P_i, C passe par R. Donc $R = P = Q$. □

Démonstration. Une cubique a dix coefficients, et la condition de passer par neuf points fixés s'exprime par un système de neuf équations linéaires homogènes en ces dix coefficients. Le système formé par les neuf équations correspondant aux neuf points d'intersection de C' et $C"$ est de rang au plus 8 : en effet, l'espace des solutions contient le plan vectoriel des $\lambda C' + \mu C"$. Il suffit donc de montrer qu'un système formé par 8 queconques de ces équations est de rang 8 : On en déduira que la neuvième équation est une combinaison linéaire des 8 autres. Géométriquement, cela veut bien dire que toute cubique qui passe par 8 des points d'intersection passe par le neuvième (une forme linéaire est combinaison linéaire d'autres formes linéaires si et seulement si son noyau contient l'intersection des noyaux de celle-ci.

Considérons donc un sous-système formé par les équations correspondant

à 8 des points d'intersection. Ces 8 équations sont indépendantes : aucune n'est combinaison linéaire des autres. On le vérifie en montrant que, pour tout point choisi parmi les 8, il existe une cubique qui contient les 7 autres, mais pas le point choisi. Cette cubique sera en fait construite comme le produit d'une droite et d'une conique.

Tout d'abord une remarque : parmi les 9 points d'intersection, il n'y en a pas 4 d'alignés, et il n'y en a pas 7 sur une conique. Sinon, on contredirait l'hypothèse que C' et C" n'ont pas de composante commune. En effet, s'il y avait 4 points d'alignés, la droite qui les contient devrait être une composante commune, d'après Bézout (Intersection d'une droite et d'une cubique). S'il y en avait 7 sur une conique et que cette conique ne se décompose pas en produit de deux droites, elle devrait aussi être une composante commune de C' et C", toujours d'après Bézout (intersection d'une conique et d'une cubique). Si la conique se décompose en produit de deux droites, une de celles-ci contient au moins 4 des 7 points, et on a vu que ceci est impossible.

Soit A le point choisi parmi les 8. On peut trouver trois points B, C, D parmis les autres, non alignés, et tels qu'aucun des cotés du triangle formé par trois de ces points ne passe par A (en utilisant qu'il n'y a pas 4 points aligné : choisir d'abord B, puis C en dehors de la droite (AB), et finalement D sur aucune des trois droite (AB), (AC), et (BC)). Parmi les coniques passant par les 4 autres points E, F, G, H, il n'y en a une unique Γ_A passant par A, une unique Γ_B passant par B, et une unique Γ_C passant par C (toujours car 4 des points ne sont jamais alignés et en utilisant ce résultat classique de géométrie projective : Cinq points du plan projectif déterminent une unique conique (éventuellement dégénérée) si et seulement s'il n'y en a pas quatre alignés). Les coniques Γ_B, Γ_C, Γ_D ne sont pas toutes les mêmes car sinon les 7 points B, C, D, E, F, G, H seraint sur une conique. Donc il y a au moins une conique parmi celles-là différente de Γ_A, et donc qui ne passe pas par A. Disons que c'est le cas pour Γ_D. Le produit de cette conique avec la droite (BC) est une cubique qui ne passe pas par A. □

Si maintenant on pose $F_1(X, Y, Z) = l(X, Y, Z)m(X, Y, Z)n(X, Y, Z)$ et $F_2(X, Y, Z) = r(X, Y, Z)s(X, Y, Z)t(X, Y, Z)$ alors notre courbe définie par $F(X, Y, Z) = 0$ passe par 8 points d'intersection de F_1 et F_2, qui sont A,B,C,D,G,V,U,O, alors, d'après le théorème les points F et W sont égaux, et ce point correspond à l'intersection de $m = 0$ et $r = 0$.

Donc, la loi ainsi définie est bien une loi de groupe sur la courbe elliptique. □

Nous avons donc démontré qu'il y avait une loi de groupe sur $C(\overline{K})$, car le théorème de Bézout s'applique sur un corps algébriquement clos. Pour passer aux points de K, nous avons donc besoin de ce théorème :

Théorème 1.5.3. *L'ensemble $E(K)$ des points rationnels d'une courbe elliptique est un groupe, muni de la même loi.*

Démonstration. Bien sûr, la seule partie à vérifier est que cette loi conserve les points rationnels.
Soient P, Q deux points rationnels de la courbe elliptique E. On note $P = (x_P, y_P, z_P)$ et $Q = (x_Q, y_Q, z_Q)$. On paramétrise la droite passant par P et Q par $M(t) = t(x_P, y_P, z_P) + (1-t)(x_Q, y_Q, z_Q)$. Cette paramétrisation a ses coefficients dans K, et on a $M(0) = P$ et $M(1) = Q$. Pour trouver le troisième point d'intersection de la droite avec la courbe, on remplace cette paramétrisation dans l'équation de la courbe. On obtient un polynôme en la variable t, de degrés 3, à coefficients dans K, dont on connaît deux racines : 0 et 1, qui sont évidemment dans K. On peut donc conclure que la troisième racine est également dans K grâce aux relations coefficients/racines, et cette racine nous donne les coordonnées du troisième point d'intersection.

Rappel 1.5.1. *Si $P(T) = aT^3+bT^2+cT+d$ avec $a \neq 0$, alors $\lambda_1+\lambda_2+\lambda_3 = -\frac{b}{a}$, où les λ_i sont les racines de P.*

□

2 Le cas complexe

2.1 Surfaces de Riemann

Définition 2.1.1. *Soit X un espace topologique séparé. Une **carte locale** de X est un couple (U, f) où U est un ouvert de X et $f : U \to \mathbb{C}$ est un homéomorphisme sur son image. Une **structure complexe** sur X est une famille de couples (U_i, f_i) telle que les U_i forment un recouvrement de X et les **applications de changements de carte** $f_i \circ f_j^{-1}$ sont holomorphes. Si X est muni d'une structure complexe, on dit que c'est une **surface de Riemann**.*

*Soient X et Y des surfaces de Riemann. $f : X \to Y$ est dite **holomorphe** si f est holomorphe dans les cartes. Autrement dit, en notant (U_i, f_i) et (U'_j, f'_j) les structures complexes sur X et Y respectivement, $f'_j \circ f \circ f_i^{-1}$ est holomorphe pour tout i,j. Les applications holomorphes sont les morphismes de la catégorie des surfaces de Riemann.*

*Une fonction $f : X \to \mathbb{C}$ non constante est dite **méromorphe** si elle se prolonge en une fonction holomorphe $X \to P^1\mathbb{C}$.*

Définition 2.1.2. *Un réseau Λ de $\mathbb{C}$ est un sous-groupe discret de $\mathbb{C}$ de la forme $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, avec $\omega_1/\omega_2 \notin \mathbb{R}$.*

Proposition 2.1.1. *Soit Λ un réseau de $\mathbb{C}$. Il existe une unique structure complexe sur le tore $\mathbb{C}/\Lambda$ telle que l'application quotient $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ soit un isomorphisme local.*

Si U est un ouvert de $\mathbb{C}/\Lambda$, on a : $f : U \to \mathbb{C}$ est holomorphe si et seulement si $f \circ \pi$ est holomorphe (au sens usuel).

Démonstration. On commence par rappeler que π est continue et ouverte.
Existence Soit $x \in \mathbb{C}$. Comme Λ est discret, on dispose d'un voisinage U_x de x tel que $\forall \omega \in \Lambda, \omega \neq 0, U_x \cap (\omega + U_x) = \varnothing$. On en déduit facilement que $\mathbb{C}/\Lambda$ est séparé : si $\pi(x)$ et $\pi(y)$ sont deux éléments de $\mathbb{C}/\Lambda$ et U_x et U_y sont deux tels voisinages de x et y disjoints ($\mathbb{C}$ est séparé), alors $\pi(U_x)$ et $\pi(U_y)$ sont des voisinages disjoints de $\pi(x)$ et $\pi(y)$.
De plus, on sait que $\mathbb{C}/\Lambda$ est compact (c'est l'image par π d'un domaine fondamental de Λ) et les projections des $(U_x)_{x\in\mathbb{C}}$ forment un recouvrement de $\mathbb{C}/\Lambda$ par des ouverts. On peut donc en extraire une famille finie (U_i). π restreinte à U_i est un homéomorphisme local. En notant $V_i = \pi(U_i)$ et $s_i : V_i \to U_i$ les sections locales de π, on obtient que (V_i, s_i) est une structure complexe sur $\mathbb{C}/\Lambda$ et π est bien un isomorphisme local car l'identité sur $\mathbb{C}$ est holomorphe.
Unicité Soient Σ et Σ' deux structures complexes sur $\mathbb{C}/\Lambda$ telles que π soit un isomorphisme local. Soit s une section locale de π sur $(\mathbb{C}/\Lambda, \Sigma)$. Alors $Id = \pi \circ s$ est (localement) holomorphe. C'est en fait un isomorphisme local. □

Proposition 2.1.2. *Soient Λ et Λ' des réseaux de $\mathbb{C}$. Alors $\mathbb{C}/\Lambda$ et $\mathbb{C}/\Lambda'$ sont isomorphes (en tant que surfaces de Riemann) si et seulement si il existe $\alpha \in \mathbb{C}$ non nul tel que $\Lambda = \alpha\Lambda'$. Dans ce cas, un isomorphisme de surfaces de Riemann est la composée d'une translation et d'un isomorphisme de groupes.*

Démonstration. Soit $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ holomorphe telle que $\phi(0) = 0$. Un résultat de topologie algébrique assure qu'il existe une unique application holomorphe $\tilde{\phi} : \mathbb{C} \to \mathbb{C}$ telle que $\tilde{\phi}(0) = 0$ et le diagramme suivant commute :

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\Lambda' \end{array}$$

Pour tout $\omega \in \Lambda$, l'application $z \mapsto \tilde{\phi}(z+\omega) - \tilde{\phi}(z)$ est continue. Or, son image est inclue dans Λ' qui est discret et $\mathbb{C}$ est connexe. Donc cette application est constante et on a :

$$\forall \omega \in \Lambda, \tilde{\phi}'(z+\omega) = \tilde{\phi}'(z)$$

$\tilde{\phi}'$ est holomorphe et doublement périodique donc constante. On intègre et on obtient $\tilde{\phi}(z) = \alpha z$. On en déduit $\alpha\Lambda \subset \Lambda'$ et on a même égalité par symétrie du raisonnement. La réciproque est triviale et les applications $z \mapsto \alpha z$ sont évidemment des morphismes de groupes. □

2.2 Fonction de Weierstrass

Soit Λ un réseau de $\mathbb{C}$.

Proposition 2.2.1. *La série*

$$\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{\omega^3}$$

converge normalement. Dans la suite, on notera

$$g_4 = 60\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{\omega^4}$$

$$g_6 = 140\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{\omega^6}$$

Démonstration. Illustration de la partie de $P(n)$ avec x, y positifs.

Soit (ω_1, ω_2) une base de Λ. Pour $n \geq 1$, on note $P(n) = \{a\omega_1 + b\omega_2; a, b \in \mathbb{R}, max(|a|, |b|) = n\}$. Les $8n$ points de Λ dans $P(n)$ sont à une distance au moins kn de 0 où k est une constante. On a donc :

$$\sum_{\omega\in\Lambda\cap P(n)}\frac{1}{|\omega|^3} \leq \frac{8}{k^3n^2}$$

Et on en déduit :

$$\sum_{\omega\in\Lambda,\omega\neq 0}\frac{1}{|\omega|^3} \leq \frac{8}{k^3}\sum_n\frac{1}{n^2} < \infty$$

□

Définition 2.2.1. *On définit la* ***fonction de Weierstrass***

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

Cette série et sa dérivée convergent normalement sur les compacts de $\mathbb{C}$ *et leurs sommes sont des fonctions méromorphes doublement périodiques (on parle aussi de* ***fonctions elliptiques****).*

Démonstration. On note (ω_1, ω_2) une base de Λ. Pour la fonction $\wp$, il suffit de remarquer que, pour $|z| \leq r$ et $|\omega| \leq 2r$, on a :

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq \frac{10r}{|\omega|^3}$$

On écrit ensuite :

$$\wp'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}$$

qui converge bien par comparaison avec $\sum \frac{1}{|\omega|^3}$ et qui est doublement périodique. En intégrant la relation de périodicité de $\wp'$ et en évaluant en $z = -\omega_1/2$, on montre que $\wp$ est doublement périodique. □

Proposition 2.2.2. *La fonction de Weierstrass vérifie l'équation différentielle suivante :*

$$\wp'^2 = 4\wp^3 - g_4\wp - g_6$$

Démonstration. En écrivant le développement en série de Laurent de chaque côté de l'égalité, on montre que la différence est holomorphe en 0, où elle vaut 0. Comme cette différence est doublement périodique, le théorème de Liouville affirme qu'elle est constante et donc nulle. □

2.3 Correspondance entre courbes et réseaux

Proposition 2.3.1. *La courbe*

$$E(\Lambda) : Y^2Z = 4X^3 - g_4XZ^2 - g_6Z^3$$

est une courbe elliptique. $E(\Lambda)(\mathbb{C})$ *est naturellement muni d'une structure complexe.*

Démonstration. La courbe affine associée à $E(\Lambda)$ a pour équation $Y^2 = 4X^3 - g_4X - g_6$. La première coordonnée d'un point singulier de la courbe sera donc une racine double du polynôme $f = 4X^3 - g_4X - g_6$. Il suffit donc de montrer que f a des racines distinctes.
On sait que $\wp'$ est doublement périodique et impaire. On en déduit que

$\wp'(\omega_1/2) = 0$. Donc $\wp(\omega_1/2)$ est racine de f. Le même raisonnement fonctionne pour $\wp(\omega_2/2)$ et $\wp((\omega_1+\omega_2)/2)$. On va maintenant montrer que ces trois nombres sont distincts.
On note D un domaine fondamental de Λ contenant 0 et $g : z \mapsto \wp(z) - \wp(\omega_1/2)$. En remarquant que $Res_P(g'/g) = ord_P(g)$, le théorème des résidus appliqué à g'/g sur le bord de D donne :

$$\sum_{P \in D} ord_P(g) = 0$$

Or, g possède uniquement un pôle double sur D qui est 0 et $\omega_1/2$ est un zéro double de g. La formule ci-dessus affirme donc que ce zéro est bien le seul. Le même raisonnement s'applique à $\wp(\omega_2/2)$ et $\wp((\omega_1+\omega_2)/2)$. □

Proposition 2.3.2. *La fonction de Weierstrass fournit une paramétrisation de $E(\Lambda)$. Plus précisément, on a un isomorphisme :*

$$\mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C})$$

$$z \neq 0 \mapsto (\wp(z) : \wp'(z) : 1)$$

$$0 \mapsto (0 : 1 : 0)$$

Remarque 2.3.1. *Cette application induit un morphisme de groupes $\mathbb{C}/\Lambda \to E(\Lambda)$*

Démonstration. **Injectivité** On a vu dans la précédente démonstration que $\wp : \mathbb{C}/\Lambda \to \mathbb{C}$ était 1 :1 sur les points $\wp(\omega_1/2)$, $\wp(\omega_2/2)$ et $\wp((\omega_1+\omega_2)/2)$. Le même raisonnement montre que cette fonction est 2 :1 sur tout autre point de son image. Or, $\wp$ est la composée de $\mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C})$ et de $x/z : E(\Lambda)(\mathbb{C}) \to \mathbb{C}$. Et cette dernière est aussi 2 :1 sur son image. On en déduit que l'application $\mathbb{C}/\Lambda \to E(\Lambda)(\mathbb{C})$ est injective.
Surjectivité Comme cette application est holomorphe, elle est continue et ouverte. Or, $\mathbb{C}/\Lambda$ est compact. Donc l'image est ouverte et compacte. Or, $E(\Lambda)$ est connexe. Donc l'application est bien surjective. □

Théorème 2.3.1. *Toute courbe elliptique sur $\mathbb{C}$ est isomorphe à une courbe $E(\Lambda)$.*

Démonstration. Soit ϕ : {réseau de $\mathbb{C}$} $\to$ {courbe elliptique sur $\mathbb{C}$}/ $\approx$, l'application $\Lambda \mapsto E(\Lambda)$. La surjectivité de ϕ est compliquée à montrer et sera admise.
ϕ est la composée de l'isomorphisme de la proposition ci-dessus avec l'application $\Lambda \mapsto \mathbb{C}/\Lambda$ qui passe au quotient par la relation $\Lambda = \alpha\Lambda'$.
On obtient : {réseaux}/$\mathbb{C}^* \approx$ {courbes elliptiques} □

3 Le théorème de Mordell-Weil

3.1 Enoncé

Définition 3.1.1. *Un **corps de nombres** est une extension finie de $\mathbb{Q}$.*

Exemple 3.1.1. $\mathbb{Q}, \mathbb{Q}[\sqrt{5}], \mathbb{Q}[i], ..$

Théorème 3.1.1. *Soient K un corps de nombres et E une courbe elliptique sur K. Alors le groupe $E(K)$ est de type fini.*

En d'autres termes, tous les points de K d'une courbe elliptique peuvent être obtenus à l'aide du procédé de tangentes et de cordes, à partir d'un nombre fini d'entre eux !

Corollaire 3.1.1. *Soit K un corps de nombres, et E/K une courbe elliptique. Alors*

$$E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$$

*L'entier r est appelé le **rang** de E/K.*

3.2 Dans le cas de $K = \mathbb{Q}$

Nous allons montrer le théorème de Mordell (1922), qui est un cas particulier du théorème de Mordell-Weil, ce qui va nous permettre de comprendre le mécanisme de la preuve.

Théorème 3.2.1. *Soit C une courbe elliptique à coefficients rationnels. Alors, $E(\mathbb{Q})$ est de type fini.*

Ici, $car(K) = car(\mathbb{Q}) = 0 \neq 2, 3$: on peut donc, sans perte de généralité, considérer une courbe elliptique mise sous forme de Weierstrass, où $f = y^2 - x^3 + ax^2 + bx + c$, avec $a, b, c \in \mathbb{Q}$. On effectue le changement de variable suivant : $x' = d^2x$, $y' = d^3y$, où d est le ppcm des dénominateurs des coefficients a, b et c, pour se ramener à une courbe elliptique avec des coefficients entiers.
Dans toute cette section, C désigne une telle courbe elliptique, et Γ désigne son groupe des points rationnels.

Pour montrer ce théorème, nous avons besoin d'introduire la notion d'hauteur, et d'utiliser plusieurs lemmes :

Définition 3.2.1. *Soit $x = \frac{m}{n} \in \mathbb{Q}$ avec $m, n \in \mathbb{Z}, m \wedge n = 1$. On définit la **hauteur** de x de la manière suivante :*
$H(x) = \max(| m |, | n |)$

Proposition 3.2.1. *Soit $N \in \mathbb{N}$ alors,*

$$\#\{x \in \mathbb{Q} \mid H(x) \leqslant N\} < \infty$$

Démonstration. Ceci vient des relations triviales suivantes :

$$| m | \leqslant \max(| m |, | n |)$$

et

$$| n | \leqslant \max(| m |, | n |)$$

Et nous n'avons donc qu'un nombre fini de possibilités pour le numérateur et le dénominateur. □

Définition 3.2.2. *Soit maintenant une courbe elliptique, mise sous forme de Weierstrass réduite : $y^2 = x^3 + ax^2 + bx + c$ avec $a, b, c \in \mathbb{Z}$.*
On définit la hauteur d'un point rationnel de la courbe $P = (x, y)$ par

$$H(P) := H(x)$$

et

$$H(O) = 1$$

Définition 3.2.3. *Soit P un point rationnel, on définit la* ***hauteur logarithmique*** *de P par $h(P) = log(H(P))$.*

Lemme 3.2.1. *Soit $P_0 \in \Gamma$ fixé. Alors, $\exists \kappa_0 = \kappa_0(a, b, c, P_0)$ telle que $h(P + P_0) \leqslant 2h(P) + \kappa_0$, $\forall P \in \Gamma$.*

Démonstration. Tout d'abord, on observe qu'en réduisant au même dénominateur, on a que le dénominateur commun à $x^3 + ax^2 + bx + c$ est celui de x^3, qui est donc égal à celui de y^2. Donc un point $P = (x, y)$, où $x = \frac{m}{q}$ avec $m \wedge q = 1$ et $y = \frac{n}{p}$ avec $n \wedge p = 1$ en choisissant p et q positifs. Alors, $q^3 = p^2$ et donc $q = e^2$ pour un certain e entier, premier à m et à n, et donc $p = e^3$. On a donc :

$$m \leqslant H(P) \ , \ e \leqslant H(P)^{\frac{1}{2}} \ , \ n \leqslant K.H(P)^{\frac{3}{2}}, K \in \mathbb{Z}$$

où la dernière inégalité vient de la substitution de $x = \frac{m}{e^2}$ dans $y^2 = x^3 + ax^2 + bx + c$ pour obtenir $n^2 = m^3 + am^2e^2 + bme^4 + ce^6 \leqslant (1 + |a| + |b| + |c|)H(P)^3$. Maintenant soit $P = (x, y)$ et $P_0 = (x_0, y_0)$ et $P + P_0 = (\epsilon, \nu)$. On veut majorer $h(P + P_0)$ avec $h(P)$. Sans perte de généralité, on peut s'abstenir de démontrer le lemme pour un nombre fini de points, quitte à augmenter κ_0 après. On choisit donc de supposer $P \neq O, P_0, -P_0$.
La droite $y = \lambda x + \mu$ qui lie P à P_0 coupe la courbe $y^2 = x^3 + ax^2 + bx + c$ en trois points dont l'abscisse x satisfait $(\lambda x + \mu)^2 = x^3 + ax^2 + bx + c$ et leur somme est l'opposé du coefficient en x^2. Il s'en suit que $x + x_0 + \epsilon = \lambda^2 - a$, où $\lambda = \frac{y - y_0}{x - x_0}$. Maintenant,

$$\epsilon = (\frac{y - y_0}{x - x_0})^2 - a - x_0 - x = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

pour des entiers A, B, C, D, E, F, G, qui ne dépendent pas de x (où y^2 a été remplacé par $x^3 + ax^2 + bx + c$, ce qui a tué le terme en x^3). Ainsi,

$$H(P+P_0) = H(\epsilon) \leqslant \max(|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|)$$
$$\leqslant \max(|AK| + |B| + |C| + |D|, |E| + |F| + |G|)H(P)^2$$

Enfin, en prenant les logarithmes, on obtient :

$$h(P + P_0) \leqslant 2h(P) + \kappa_0.$$

□

Lemme 3.2.2. *Il existe une constante $\kappa = \kappa(a, b, c)$ telle que $h(2P) \geq 4h(P) - \kappa$, $\forall P \in \Gamma$.*

Démonstration. On pose $P = (x, y)$ et $2P = (\epsilon, \nu)$. Sans perte de généralité, on prend $2P \neq O$. Comme avant, on a $2x + \epsilon = \lambda^2 - a$, où $\lambda = \frac{\partial Y}{\partial X}(P) = \frac{3x^2+2ax+b}{2y}$ et donc

$$\epsilon = \lambda^2 - a - 2x = \frac{x^4 + ...}{4x^3 + ...}$$

et le numérateur et le dénominateur n'ont pas de racine commune car la courbe est elliptique et donc non singulière.
Nous avons maintenant besoin de ce lemme :

Lemme 3.2.3. *Soit $f(x), g(x) \in \mathbb{Z}[x]$ deux polynômes sans racine commune dans $\mathbb{C}$. Soit d le maximum de leur degrés. Alors, si $r \in \mathbb{Q}$, $g(r) \neq 0$, alors :*

$$dh(r) - \kappa \leqslant h(\frac{f(r)}{g(r)}) \leqslant dh(r) + \kappa$$

pour une certaine constance κ qui dépend de f et de g.

Démonstration. Comme $f \wedge g = 1$, ils existent $u, v \in \mathbb{Q}(x)$ tels que $u(x)f(x) + v(x)g(x) = 1$. Pour $r = \frac{m}{n}$ (avec $m \wedge n = 1$), soit $F(r) = n^d f(r)$ et $G(r) = n^d g(r)$, de sorte que $F(r)$ et $G(r)$ sont des entiers. Maintenant, $u(r)F(r) + v(r)G(r) = n^d$. Soit A le ppcm des dénominateurs des coefficients de u et v et soit e le maximum de leurs degrés. Alors, $An^e u(r)$ et $An^e v(r)$ sont entiers, et ainsi $F(r) \wedge G(r) | An^{d+e}$. Aussi, on suppose $f(x) = a_0 x^d + ... + a_d$ avec $a_0 \neq 0$, alors $F(r) = a_0 m^d + ... + a_d n^d$ et $n \wedge F(r) | a_0$ et $F(r) \wedge G(r) | A a_0^{d+e}$. Soit $R := A a_0^{d+e}$. On a :

$$H(\frac{f(r)}{g(r)}) = H(\frac{F(r)}{G(r)}) \geqslant \frac{1}{R} \max(|F(r)|, |G(r)|)$$

Cela nous donne :

$$\frac{H(\frac{f(r)}{g(r)})}{H(r)^d} \geqslant \frac{\max(|F(r)|, |G(r)|)}{R \max(|m|^d, |n|^d)} = \frac{\max(|f(r)|, |g(r)|)}{R \max(|r|^d, 1)}$$

La partie de droite est minorée par une constante positive C (car une limite finie non nulle quand r tend vers l'infini (en fait égale à a_0/R, et un minimum non nul sur tout compact car f et g ne s'annulent pas simultanément). Alors,

$$H(\frac{f(r)}{g(r)}) \geqslant C.H(r)^d$$

et

$$h(\frac{f(r)}{g(r)}) \geqslant dh(r) - \kappa$$

comme voulu. L'autre inégalité n'est pas nécessaire dans notre cas. □

□

Lemme 3.2.4. *2Γ est d'indice fini dans Γ.*

Démonstration. Nous ne traitons que le cas particulier où il y a un point rationnel $(x_0, 0)$ d'ordre 2. Afin de ramener ce point en $(0,0)$, on effectue un changement de variable et on ramène l'équation à $y^2 = x^3 + ax^2 + bx$. (Cette courbe a pour discriminant $b^2(a^2 - 4b)$ qui est non nul car la courbe est lisse.) Si C a pour équation $y^2 = x^3 + ax^2 + bx$, on définit $\tilde{C}$ la courbe d'équation $y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x$ où $\tilde{a} = -2a$ et $\tilde{b} = a^2 - 4b$. On remarque que $(x, y) \in \tilde{\tilde{C}}$ si et seulement si $(x/4, y/8) \in C$. On définit $\phi : C \to \tilde{C}$ telle que $\phi : (x, y) \mapsto (\tilde{x}, \tilde{y})$ où $\tilde{x} = x + a + b/x$ et $\tilde{y} = y(1 - b/x^2)$ et $(0,0)$ et O sont envoyés sur $\tilde{O}$. ϕ est un morphisme de groupes de noyau $\{(0,0); O\}$.
On définit $\psi : \tilde{C} \to C$ comme la composée de $\tilde{\phi}$ et $(x, y) \mapsto (x/4, y/8)$. ψ est un morphisme de groupe de noyau $\{(0,0); O\}$. La composition de ϕ et ψ est l'application $P \mapsto 2P$.
Afin de montrer le lemme, il suffit donc de montrer que $\phi(\Gamma)$ est d'indice fini dans $\tilde{\Gamma}$ et que $\psi(\tilde{\Gamma})$ est d'indice fini dans Γ. Par symétrie de l'argument, il suffit donc de montrer le dernier fait.
On a $\tilde{x} = 0$ si et seulement si $y = 0$, c'est à dire $x(x^2 + ax + b) = 0$ avec $x \neq 0$, ce qui équivaut à : $a^2 - 4b$ est un carré.
Si $\tilde{x} = r^2$, $(\tilde{x}, \tilde{y}) \in \phi(\Gamma)$. En effet, $(\tilde{x}, \tilde{y}) = \phi(\frac{1}{2}(r^2 - a + \frac{\tilde{y}}{r}), \frac{r}{2}(r^2 - a + \frac{\tilde{y}}{r}))$. La réciproque est évidente.
Soit $\mathbb{Q}^{*2}$ le sous-groupe de $\mathbb{Q}^*$ constitué des carrés. On définit $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ par $(x, y) \mapsto x$ si $x \neq 0$, $(0,0) \mapsto b$, $O \mapsto 1$. α est un morphisme de groupes. En effet, on suppose que $P_1 + P_2 + P_3 = O$.
Premier cas : on suppose que P_1, P_2 et P_3 sont alignés sur une droite d'équation $y = \lambda x + \mu$. Soient x_1, x_2 et x_3 les racines de $(\lambda x + \mu)^2 = x^3 + ax^2 + bx$. On a : $\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = \mu^2 = 1$ dans $\mathbb{Q}^*/\mathbb{Q}^{*2}$.
Deuxième cas : Si $P_1 = (0,0)$, alors $\mu = 0$ et x_2 et x_3 sont racines de $\lambda^2 x = x^2 + ax + b$ et $\alpha(P_1)\alpha(P_2)\alpha(P_3) = bx_2x_3 = b^2 = 1$ dans $\mathbb{Q}^*/\mathbb{Q}^{*2}$.
Troisième cas : si $P_1 = O$, alors $P_2 = -P_3$ et $x_2 = x_3$ et $\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_2x_3 = 1$ dans $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

De plus, l'image de α est finie car contenue dans l'ensemble des diviseurs de b. En effet, soit $P = (\frac{m}{e^2}, \frac{n}{e^3}) \in C$. Alors $\alpha(P) = m$. On a : $n^2 = m(m^2 + ame^2 + be^4)$ donc tout diviseur premier de m apparaît comme une puissance paire dans m tandis qu'il apparaît comme une puissance impaire dans $(m^2 + ame^2 + be^4)$ donc dans be^4 donc dans b car m et e sont premiers entre eux.
Il est alors clair que le noyau de α est exactement l'image de ψ. Par conséquent, α induit un isomorphisme de $\Gamma/\psi(\tilde{\Gamma})$ dans un sous-groupe fini de $\mathbb{Q}^*/\mathbb{Q}^{*2}$. En particulier, $\Gamma/\psi(\tilde{\Gamma})$ est fini. □

Nous pouvons à présent démontrer le théorème de Mordell.

Démonstration. On choisit $Q_1, ..., Q_n$ des représentants des classes de $\Gamma/2\Gamma$. Soit $P \in \Gamma$. On peut écrire : $P = 2P_1 + Q_{i_1}$ puis $P_1 = 2P_2 + Q_{i_2}$ etc. On définit ainsi une suite (P_m) de points de Γ. On pose κ' la plus grande des constantes $\kappa_0(a, b, c, -Q_i)$. On obtient : pour tout P, Q_i, $h(P - Q_i) \leq 2h(P) + \kappa'$. Et donc :

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_i) + \kappa \leq 2h(P_{j-1}) + \kappa + \kappa'$$

donc $h(P_m) \leq \kappa + \kappa'$ à partir d'un certain rang (en effet, la suite $h(P_n) - (\kappa + \kappa')/2$ est majorée par une suite géométrique de raison $1/2$). Dans ces conditions, l'ensemble

$$\{Q_1, ..., Q_m\} \cup \{P; h(P) \leq \kappa + \kappa'\}$$

est fini et génère Γ. □

3.3 Cas général

Passons maintenant au théorème de Mordell-Weil. Nous n'allons pas donner ici les preuves, mais uniquement les étapes nécessaires pour montrer ce théorème. Toute personne intéressée par la preuve formelle pourra se référer au livre de Silverman. Nous avons besoin d'une généralisation du lemme 3.2.4 : du cas $K = \mathbb{Q}$ à un corps de nombres quelconque. C'est en fait le théorème faible de Mordell-Weil. Ensuite, nous allons introduire une fonction correspondant à la fonction **hauteur** de la partie précédente, qui vérifie les mêmes propriétés énoncées dans les précédents lemmes. Avec ces deux généralisations, nous allons pouvoir montrer le théorème qui nous intéresse.

Théorème 3.3.1. *(Théorème faible de Mordell-Weil)*
Soit K un corps de nombres. Soit E une courbe elliptique sur K. Le groupe $\Gamma = E(K)/mE(K)$ est fini, $\forall m \geq 2$.

Maintenant armés de ce théorème, nous devons définir quelques notions pour arriver à ce qui nous intéresse.

Proposition 3.3.1. *La procédure de descente :*
Soit A un groupe abélien. On suppose qu'il existe une fonction "hauteur" $h : A \to \mathbb{R}$ telles que :
1) Soit $Q \in A$. Il existe une constante C_1 qui dépend de A et Q telle que :

$$\forall P \in A : h(P+Q) \leq 2h(P) + C_1$$

2) Il existe un entier $m \geq 2$ et une constante C_2, qui dépend de A tels que :

$$\forall P \in A : h(mP) \geq m^2 h(P) - C_2$$

3) Pour toute constante c_3, l'ensemble $\{P \in A \mid h(P) \leq C_3\} est fini.$
Alors nous avons le résultat suivant :

$$Si\ \frac{A}{mA} est\ fini,\ alors\ A\ est\ de\ type\ fini$$

Il nous reste donc à montrer que pour toute courbe elliptique et pour tout corps de nombres K, nous pouvons trouver une telle fonction h, ce qui conclura le théorème.

Nous avons maintenant besoin d'introduire le degré local :

Définition 3.3.1. *Soit K un corps. On appelle* ***valuation*** *une fonction :*

$$v : A \to \mathbb{R}$$

qui vérifie :

$$\forall x \in A\ ,\ v(x) = \infty \Leftrightarrow x = 0$$

$$\forall x, y \in A\ ,\ v(xy) = v(x) + v(y)$$

$$\forall x, y \in A\ ,\ v(x+y) \geq \min(v(x), v(y))$$

Notation 3.3.1. *Dans cette section, K est un corps de nombres, M_K est l'ensemble des valuation sur K. On note K_v le complété de K, par rapport à la valuation v.*

Définition 3.3.2. *Soit K un corps de nombres et $v \in M_K$ une valuation. On apelle le* ***degré local*** *la quantité : $n_v = [K_v : \mathbb{Q}_v]$.*

Définition 3.3.3. *On définit alors une fonction hauteur sur $P^n(K)$ comme suit : Pour $p = [x_0, ..., x_n] \in P^n(K)$:*

$$H_k(P) = \prod_{v \in M_K} \max(|x_0|_v, ..., |x_n|_v)^{n_v}$$

Cette fonction dépend a priori du corps K. En fait, on peut montrer que pour $L/K/\mathbb{Q}$ une extension de corps de nombres, on a :

$$H_L(P) = H_K(P)^{[L:K]}$$

On définit alors la fonction H, qui ne dépend pas du corps de nombre choisi :

$$H(P) = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$$

On définit enfin la fonction hauteur, qui vérifie les hypothèses souhaitée comme étant :

$$h(P) = log(H(P))$$

.

Et on prouve ainsi le théorème en utilisant la procédure de descente.

To sum up

In this document, we needed to recall some basic algebraic properties, in order to introduce the defintion of elliptic curve, the main object of our subjet. To study those curves, we needed to switch from the affine representation to the projective one, and reciprocally. We saw that we can define a group law on this kind of curves, which is really useful to work with. We illustrated this law thanks to some drawing. Then we spoke about the link with the complex numbers. Indeed, elliptic curves are initially defined on $\mathbb{C}$. The definition on another field is a spread of the complex case. The complex elliptic curves are defined as tori and got by a quotient of $\mathbb{C}$ by a lattice. We show that the definitions match : all the elliptic curves algebrically defined on $\mathbb{C}$ are torus (as a surface and as a group).
Finally, we stated Mordell-Weil's theorem, and proved the Mordell one, in the case $K = \mathbb{Q}$.

Conclusion

Finalement, nous avons commencé par définir les courbes elliptiques comme des cubiques projectives lisses. Nous avons ensuite expliqué comment les étudier dans l'affine. Par la suite, nous nous intéressons à l'ensemble des points de la courbe à coordonnées dans un corps fixé. On muni cet ensemble d'une loi de groupe abélien. On montre que, dans le cas de $\mathbb{C}$, ce groupe est un tore complexe. Puis on annonce le théorème de Mordell-Weil : dans le cas d'un corps de nombres, ce groupe est finiment engendré. Nous pouvons donc donner sa structure.

En approfondissant le sujet, on se rend compte que la théorie des courbes elliptiques peut servir pour montrer des théorèmes très importants, comme le grand théorème de Fermat, qui est resté une conjecture pendant 350 ans. L'énoncé est le suivant : si r est un entier au moins égal à 4, toute solution en entiers a, b et c de l'équation $a^r + b^r = c^r$ est triviale, c'est-à-dire que a, b ou c est nul. L'idée est d'associer à une solution non triviale de $a^r + b^r = c^r$ la courbe elliptique $E_{ab} : Y^2 = X(X - a^r)(X + b^r)$. Le discriminant de cette courbe vaut abc^{2r}. Le point majeur de cette démarche est que cette courbe auraient tellement de bonnes propriétés qu'elle ne pourrai exister.

Comme nous l'avons dis dans l'introduction, les courbes elliptiques interviennent dans de nombreux autres domaines et sont extrêmement utiles, en cryptographie par exemple. Voilà donc l'intérêt de travailler sur cette notion très intéressante !

Bibliographie

-J.S. Milne. Elliptic Curves.Kea Books. 2006

-Robin Hartshorne. Algebraic Geometry. Springer-Verlag New York, 1977.

-Joseph H. Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag, New York, 1986.

-Alvaro Lozano-Robledo. Elliptic Curves, Modular forms, and their L-functions. 2011.